Unsolvable Systems of Equations and Proof Complexity

Toniann Pitassi[1]

Abstract. This abstract discusses algebraic proof systems for the propositional calculus. We present recent results, current research directions, and open problems in this area.

1991 Mathematics Subject Classification: Primary 03F, 68Q, 68R05, 20C30, 14Q99
Keywords and Phrases: Systems of polynomial equations over finite fields, propositional proof complexity, lower bounds, Grobner bases.

1 Introduction

A fundamental problem in logic and computer science is understanding the efficiency of propositional proof systems. It has been known for a long time that $NP = coNP$ if and only if there exists an efficient propositional proof system, but despite 25 years of research, this problem is still not resolved. (See [21] for an excellent survey of this area; see also [2] for a more recent article focusing on open problems in proof complexity.) The intention of the present article is to discuss algebraic approaches to this problem. Our proof systems are simpler than classical proof systems, and purely algebraic. It is our hope that by studying proof complexity in this light, that new upper and lower bound techniques may emerge. This paper is a revision and update of the earlier paper ([18]); due to space considerations, we omit all proofs and focus on current research directions.

Let $C = C_1 \wedge C_2 \wedge ... \wedge C_m$ be an instance of the classical NP-compete problem, 3SAT. That is, C is a propositional formula over $\{x_1, ..., x_n\}$, in conjunctive normal form, where each C_i is a clause of size at most three. Each clause C_i can be converted into an equation, $\overline{C_i} = 1$ over F such that C is unsatisfiable if and only if $\{\overline{C}_1 = 0, ..., \overline{C}_m = 0\}$ has no $0/1$ solution. The equations $Q = \{Q_1 = 0, ...Q_R = 0\}$ corresponding to C are: $\{\overline{C}_1 = 0, ..., \overline{C}_m = 0\}$, plus the equations $x^2 - x = 0$ for all variables x.

We show how to translate from the basis $\{\vee, \wedge, \neg\}$ to the basis $\{+, \times, 1\}$ over a field F. For a atomic, $t(a) = 1 - a$; $t(\neg x) = 1 - t(x)$; $t(x \vee y) = t(x)t(y)$; and lastly, $t(x \wedge y) = t(\neg(\neg x \vee \neg y) = t(x) + t(y) - t(x)t(y)$. Our translation has the property that for any truth assignment α, and any boolean formula f, f evaluates

[1]Supported by NSF NYI grant CCR-9457783, US-Israel BSF Grant 95-00238, and Grant INT-9600919/ME-103 from NSF and MŠMT (Czech Republic)

to 1 under α if and only if $t(f)$ evaluates to 0 under α. In other words, "0" represents true over the new basis. Moreover, one could further convert Q into a family of degree 2 equations by replacing each monomial xyz in Q_i by xw (where w is a new variable), and adding the extra equations $w - yz = 0$ and $w^2 - w = 0$.

The above reduction (due to Valiant [22]) shows that solving systems of degree 2 polynomial equations is NP-complete. We are interested in defining natural algebraic proofs in the case where the equations are unsolvable, and in studying the complexity of the resulting proofs. What exactly is a natural algebraic proof, and how long can such proofs be? Our starting point for defining such algebraic proof systems is Hilbert's Nullstellensatz. That is, if $Q_i(\overline{x}) = 0$ is a system of algebraic equations over F (translated from an instance of 3SAT), then the equations do not have a solution in the algebraic closure of F if and only if there exists polynomials $P_i(\overline{x})$ from $F[\overline{x}]$ such that $\sum_i P_i(\overline{x})Q_i(\overline{x}) = 1$. We can think of the polynomials P_i as a *proof* of the unsolvability of the equations Q_i. Moreover, in our scenario since Q_i includes the equations $x^2 - x = 0$ for all variables x, there exists a solution if and only if there exists a $0-1$ valued solution. This is the main property which distinguishes our investigations from earlier, classical work on the effective Nullstellensatz. ([10, 15, 5]).

Algebraic proof systems are appealing because of their simplicity and non-syntactic nature. Moreover, the question of how large a proof must be amounts to asking how many field operations are required in order to generate the constant polynomial from certain initial polynomials. Moreover these proof systems are powerful, and by studying various complexity notions (degree, monomial size, algebraic size), there are close correspondences between these systems and various classical propositional proofs.

The organization of the paper is as follows. In Section 2, we define our algebraic proof systems and various complexity measures on them. In Section 3, we state basic theorems about algebraic proofs and simulation results. In Section 4, we focus our attention on lower bounds. Lastly in Section 5, we present several open problems in this area.

2 Algebraic Proof Systems

Recall that $C = C_1 \wedge C_2 \wedge ... \wedge C_m$ is a propositional formula over $\{x_1, ..., x_n\}$, in conjunctive normal form, where each C_i is a clause of size at most three. Let Q be the corresponding system of (degree 3) polynomial equations. Here is a simple example. Let $C = (b \vee a) \wedge (\neg a \vee b) \wedge (\neg b)$. Then $Q = \{Q_1, Q_2, ..., Q_5\}$, where $Q_1 = (1-b)(1-a) = 1-a-b+ab$, $Q_2 = (a)(1-b) = a - ab$, $Q_3 = b$, $Q_4 = a^2 - a$, $Q_5 = b^2 - b$.

An *algebraic* refutation for C (over a fixed ring or field F) is an algebraic straight-line program, $S = S_1, ..., S_l$ such that each S_i is either one of the initial equations (from Q) or is obtained from previous equations by a valid rule, and where the final equation S_l is $0 = 1$. The two rules are as follows. (1) From $g_1(\overline{x}) = 0$ and $g_2(\overline{x}) = 0$, derive $ag_1(\overline{x}) + bg_2(\overline{x}) = 0$, where a, b are constants from F; (2) From $g(\overline{x}) = 0$, infer $xg(\overline{x}) = 0$ for x a variable. (Thus, a proof is merely an explicit derivation that 1 is in the ideal generated by Q.) In the above example, a refutation is: $S_1 = Q_1$, $S_2 = Q_2$, $S_3 = Q_3$, $S_4 = S_1 + S_2 = 1 - b$, $S_5 = S_4 + S_3 = 1$. An algebraic refutation S for Q can also be put in an alternate form, $\sum_i P_i(\overline{x})Q_i(\overline{x}) = 1$.

Our algebraic proof system is *sound* since such a straight-line program is not possible to obtain if Q is solvable. The algebraic proof system is also *complete* since every unsolvable system of equations Q (derived from an unsatisfiable 3CNF formula C) has an algebraic proof. There are several proofs of completeness. One follows from (the weak form of) Hilbert's Nullstellensatz. There are also other simpler and more constructive proofs [18, 8]; one is obtained by simulating a truth-table proof and a second is by simulating a type of tableau proof.

2.1 Complexity measures

We will discuss several complexity measures on algebraic refutations. Perhaps the most natural is the *algebraic size*. This is defined to be the number of lines, l, in S. The *degree* is defined to be the maximum degree of the intermediate polynomials S_i, after simplifications. This measure has been studied quite a bit, and the name *Polynomial Calculus* (PC) is given to algebraic proofs in this form, where the S_i's are viewed as explicit sums of monomials. Another degree measure, which is called the *Nullstellensatz* (HN) degree is the maximum degree of the intermediate polynomials S_i *before* simplifications. That is, the maximum degree of the polynomial $\sum_i P_i Q_i$ in the alternate representation $\sum_i P_i Q_i = 1$.

Note that the minimal Polynomial Calculus degree of a formula f is never greater than the minimal Nullstellensatz degree of f; however, the Polynomial Calculus degree can sometimes be much smaller as is evidenced by the following example. Let IND_n denote the following system of degree 2 equations: (1) $1-x_1 = 0$; (2) $x_i(1-x_{i+1}) = 0$ for all $1 \le i \le n-1$; (3) $x_n = 0$ and (4) $x_i^2 - x_i = 0$ for all $1 \le i \le n-1$. (These equations formalize induction: if $x_1 = 1$ and $x_n = 0$, then there must be an index i such that $x_i = 1$ and $x_{i+1} = 0$.) It is not too hard to see (by applying induction!) that these equations have a degree 2 PC refutation; on the other hand, they require degree $O(logn)$ Nullstellensatz refutatons [7].

2.2 Automatizability

An important issue in proof complexity is whether or not a given proof system can actually be used as the basis for an efficient automated theorem prover. Intuitively, it seems that the more expressive and powerful the proof system, the harder it is to perform an efficient search for a short proof. A proof system S is thus said to be *automatizable* if there exists a deterministic procedure A that takes as input a (unsatisfiable) formula f and outputs an S-proof f in time polynomial in the size of the shortest S-proof of f. In other words, if S is automatizable, then short proofs can be found efficiently.

One of the nicest features of algebraic proofs is that small degree proofs can be found quickly–in other words, small-degree proofs are automatizable. To see this in the case of small-degree Nullstellensatz proofs, note that if $\sum_i P_i Q_i = 1$ where P_i's have degree at most d, and the Q_i's have degree at most 3, then the total number of monomials on the left side is bounded by a polynomial in d and therefore we can set up a system of linear equations (one for each monomial) and solve for the coefficient values in polynomial time. Using a modification of the Gröbner basis algorithm, [11] have shown that small-degree Polynomial Calculus proofs are also automatizable.

THEOREM. [11] For all d, n, there is an algorithm A such that for any (unsatisfiable) 3CNF formula f with underlying variables $x_1, .., x_n$, A returns a degree-d Polynomial Calculus refutation (if one exists) in time $n^{O(d)}$.

3 RELATIONSHIP TO CLASSICAL PROOF SYSTEMS

In this section, we will discuss the relationship between the size of algebraic proofs under the above complexity measures and the size of more standard propositional proofs.

3.1 ALGEBRAIC PROOFS VERSUS FREGE PROOFS

DEFINITION. The algebraic proof system over F is *polynomially-bounded* if there exists a constant c such that for every unsatisfiable 3CNF formula, f, there exists an algebraic proof of f of size $O(|f|^c)$ (that is, the proof is of size polynomial in the size of f).

The standard definition of a propositional proof system is as follows.

DEFINITION. Let $L \subseteq \Sigma^*$, where Σ is a finite alphabet, and Σ^* denotes all finite strings over Σ. (Typically, L encodes either the set of all tautological formulas, or the set of all unsatisfiable formulas.) Then a Cook-Reckhow proof system for L is a function $f : \Sigma^* \rightarrow L$, where f is an onto, polynomial-time computable function. A Cook-Reckhow proof system, f, is polynomially bounded if there is a polynomial $p(n)$ such that for all $y \in L$, there is an $x \in \Sigma^*$ such that $y = f(x)$ and $|x|$ (the length of x) is at most $p(|y|)$.

A key property of a Cook-Reckhow proof system is that, given an alleged proof, there is an efficient method for checking whether or not it really is a proof. For most standard, axiomatic proof systems (Extended Frege, Frege, even ZFC), there is actually a very efficient method for checking whether or not it is really a proof. This property leads to the following theorem.

THEOREM. [13] There exists a polynomially-bounded Cook-Reckhow propositional proof system if and only if $NP = coNP$.

The above theorem does not appear to hold for algebraic proofs because there is no known deterministic polynomial time algorithm to check whether or not a polynomial is identically 1, even in the case of finite fields. (In other words, there is no efficient procedure to check that it is a proof.) Nonetheless, the probabilistic polynomial-time algorithm due to Schwartz allows us to prove that if algebraic proofs are polynomially-bounded, then the polynomial hierarchy collapses.

THEOREM. [18] For any prime p, if the algebraic proof system over Z_p is polynomially-bounded, then $PH = \Sigma_2^p$.

We conjecture that the above premise also implies $NP = coNP$. It is not too hard to show that algebraic proof systems are at least as powerful as Extended Frege systems, as is evidenced by the following theorem.

THEOREM. [18] For any commutative ring R, Frege proofs (and Extended Frege proofs) can be polynomially simulated by algebraic proofs with polynomial size.

It is open whether or not the simulation holds in the reverse direction.

3.2 POLYNOMIAL CALCULUS VERSUS RESOLUTION

Resolution proofs dominate the work in automated theorem proving since they are extremely simple and can also be applied to first order theorem proving. A Resolution proof P of an (unsatisfiable) CNF formula $f = C_1 \wedge ... \wedge C_m$ is a sequence of clauses $D_1, ..., D_l$ such that: (a) each D_i is either an initial clause from f or follows from two previous clauses by the Resolution rule, and (b) the final clause D_l is the empty clause. The resolution rule derives $(A \vee B)$ from $(A \vee x)$ and $(B \vee \neg x)$, where A and B are disjunctions of literals. The size of the above Resolution proof is l; a tree-like proof has the additional property that each intermediate clause generated in the proof (not including the initial clauses) can be used at most once in the derivation–i.e., if it is used more than once it must be re-derived. Tree-like Resolution is of practical interest since most theorem provers are based on tree-like Resolution proofs. The following theorem gives a relationship between small degree Polynomial Calculus proofs and small-size Resolution proofs.

THEOREM. [11] If f has a tree-like Resolution proof of size S, then f has a degree $O(logS)$ Polynomial Calculus refutation. If f has a Resolution proof of size S, then f has a degree $O(\sqrt{nlogS})$ Polynomial Calculus refutation.

The intuition behind the above proof is as follows. Define the *width* of a Resolution proof to be the maximum clause size in the proof. The proof of the above theorem can be used to show: (1a) If f has a size S tree-like Resolution proof, then f has a width $O(logS)$ Resolution proof [9]; (1b) if f has a size S Resolution proof, then f has a width $O(\sqrt{nlogS})$ Resolution proof. And secondly, it is easy to show: (2) if f has a width d Resolution proof, then f has a degree $O(d)$ Polynomial Calculus proof.

3.3 POLYNOMIAL CALCULUS VERSUS BOUNDED-DEPTH FREGE

Bounded-depth Frege proofs are Frege proofs where the depth of each intermediate formula is bounded by a fixed constant. (See [21, 2] for motivation and details.) Bounded-depth Frege proofs are known to be strictly more powerful than Resolution, but strictly less powerful than unrestricted Frege proofs. $AC^0[p]$-Frege proofs are bounded-depth Frege proofs where the underlying connectives are: unbounded fanin AND, OR, NOT and MODp. There are no nontrivial lower bounds known at present for $AC^0[p]$-Frege proofs, and the original motivation for defining and studying small-degree algebraic proofs was to prove such lower bounds [4].

It does not seem to be possible to simulate polynomial-size $AC^0[p]$-Frege proofs by small degree Polynomial Calculus proofs (over GF_p). This is because any single unbounded fanin OR gate would translate into a large degree polynomial. To circumvent this problem, [8] extended the Polynomial Calculus by adding new equations to the initial ones, where these new equations introduce new variables to represent or define unbounded fanin OR gates. The new equations, R, are small-degree polynomial equations in the original variables, plus the new "extension variables." The nesting level of the new equations corresponds to the depth of the unbounded fanin formulas that can be represented. Thus, loosely speaking, a degree d constant-depth Polynomial Calculus with Extension proof of f is a degree d Polynomial Calculus refutation of $0 = 1$ from the equations Q, R, where Q corresponds to the original equations defining f, and R corresponds to the new extension axioms, and such that the definitions given by R have a constant number of levels of nestings. With these definitions, [8] show that constant-depth $AC^0[p]$-Frege proofs are essentially equivalent to constant-depth Polynomial Calculus with Extension proofs.

In a different line of work, [17] show that any quasipolynomial-size $ACC^0[2]$-Frege proof can be simulated by a quasipolynomial-size, depth 3 Frege proof of a very special form: the output gate is a weak threshold gate, the middle layer consists of mod 2 gates and the input layer consists of AND gates of small fanin. Put another way, each formula in the depth 3 Frege proof is a probabilistic small-degree polynomial over GF_2. This in turn can be viewed as another generalization of small-degree Polynomial Calculus proofs.

4 Lower Bounds

In the last five years, there have been many lower bounds obtained on the degree of Nullstellensatz and Polynomial Calculus proofs of various principles. The table below summarizes the progress thus far. Of particular importance are the formulas expressing the pigeonhole principle, and the formulas expressing various counting principles.

The onto version of the propositional pigeonhole principle states that there is no 1-1, onto map from m to n, $m > n$. This can be expressed by the following equations, with underlying variables $P_{i,j}$, $i \leq m$, $j \leq n$: (1) $P_{i,1} + ... + P_{i,n} - 1 = 0$, for all $i \leq m$; (2) $P_{1,j} + ... + P_{m,j} - 1 = 0$, for all $j \leq n$; and (3) $P_{i,k}P_{j,k} = 0$, for all $i, j \leq m$, $k \leq n$. For each n, let the above set of equations be denoted by $\neg PHP^{m,n}_{onto}$. For each $m = n + 1$, there is a constant degree Nullstellensatz proof over GF_p of $\neg PHP^{m,n}_{onto}$. The proof is obtained by adding together all of the above equations in (1) and subtracting all of the above equations in (2). Each variable will cancel because it occurs once positively in (1) and once negatively in (2), and we are left with $m - n = 1$. However, for $m = nmodp$, this proof fails.

The more general version of the propositional pigeonhole principle states that there is no 1-1 map from m to n. For each $m > n$, the general pigeonhole principle can be expressed by equations (1) and (3) above, and is denoted by $\neg PHP^{m,n}$.

The mod q counting principle, Mod^q_n, states that there is no way to partition a set of size n into equivalence classes, each of size exactly q. For each n, the negation of this principle ($\neg Mod^q_n$) can be expressed by the following equations, with underlying variables X_e, $e \subseteq [1,..,m]$, $|e| = q$, $m = pn + 1$:

(1) $\sum_{e,\ i\in e} X_e - 1 = 0$, for all $i \leq m$; (2) $X_e X_f = 0$, for all e, f, $e \cap f \neq 0$.

The induction principle was explained earlier. The principle Homesitting is a variant of strong induction. The principle Graph, stands for Tseitin's graph tautologies: given a connected graph, where each vertex has a 0-1 labelling (charge) and such that the mod 2 sum of all labellings is odd, the principle states that the mod 2 sum of the edges coming into each vertex is equal to the charge of that vertex. Clearly this principle is unsatisfiable and when the underlying graphs are k-regular and have good expansion properties, the associated formula is hard to prove (as long as the field does not have characteristic 2). Subsetsum is a single equation, $m - \sum_i (c_i x_i) = 0$ and this lower bound shows that over fields of characteristic 0, there are no small Nullstellensatz degree refutations of the subset sum principle. HN means that the degree lower bound holds for Nullstellensatz; PC means that the degree bound holds in the stronger Polynomial Calculus.

By now, there are many families of formulas requiring large Nullstellensatz degree, but a lack of many explicit lower bounds for Polynomial Calculus degree. The first such lower bound for the Polynomial Calculus is the paper by Razborov [19]. In that paper, he explicitly describes the set of all polynomials derivable from the initial equations in degree d. The only other lower bound known for the Polynomial Calculus, due to Krajíček[16], uses important ideas from Ajtai [1] linking the lower bound in question to the representation theory of the symmetric group.

Formulae	Reference	Lower bound	Notes
PHP	[12]	$O(n^{1/4})$ (HN)	nearly optimal
PHP	[19]	$O(n^{1/2})$ (PC)	nearly optimal
ontoPHP	[3]	$O(n)$ (HN)	nearly optimal
IND	[7]	$O(logn)$ (HN)	nearly optimal
Homesitting	[11, 6]	$O(n^{1/2})$ (HN)	
Graph	[14]	$O(n)$ (HN)	$Char(F) \neq 2$
Modp	[4, 1]	nonconstant (HN)	
Modp	[8]	$n^{\Omega(1)}$ (HN)	
Modp	[16]	nonconstant (PC)	
Subsetsum	[8]	$O(n)$ (HN)	$Char(F) = 0$

4.1 The Design Method

In this section we review the primary method that has been used to obtain the above Nullstellensatz degree lower bounds.

Let R be any commutative ring, and let $\mathcal{Q} = \{Q_1, .., Q_m\}$ be a set of unsolvable equations of degree at most 3 over $R[x_1, ..., x_n]$, where m is $n^{O(1)}$. We want to show that there is no degree d set of polynomials $P_1, ..., P_m$ such that $\sum_i P_i Q_i = 1$. Assume for sake of contradiction that degree d P_i's do exist. Write P_i as $\sum_m a^i_m X_m$, where $m \in \{0,1\}^n$, X_m is the corresponding monomial, and a^i_m is the coefficient in front of that monomial in P_i. Because the total number of monomials in the P_i's is bounded by $n^{O(d)}$, we can write a system of linear equations with the coefficients a^i_m as variables such that the system of linear equations has a solution if and only if such P_i's exist. In particular, the condition $\sum_i P_i Q_i = 1$ can be specified by a system of linear equations in the a_i^m's where for each nonempty monomial m of degree at most $d+3$, we have one equation specifying that the sum of all coefficients in front of this monomial must be 0, and for the empty monomial, we have one equation specifying that the sum of all coefficients in front of the empty monomial must be 1.

Now by weak duality, if we can find a linear combination of the equations such that the left-hand-side of the linear combination is 0, then there can be no solution. (Because the total sum of the right-hand-sides of the equations is 1.) Conversely, if R is a field, then we get the converse direction as well. The name *design* refers to the linear combination of the equations witnessing the fact that the equations can have no solution; because of the structure of the original Q_i's, the properties required of the linear combination can often be seen to be equivalent to the existence of a particular type of combinatorial property, and thus it is called a design.

5 Open Problems

5.1 Lower bounds for stronger proof systems

The most outstanding question is to strengthen these methods to obtain lower bounds for stronger systems, such as $AC^0[2]$-Frege proofs. A solution to this problem seems to be within reach. For this system, a candidate hard tautology is the principle Mod_p^n for p prime.

5.2 Degree lower bounds

Lower bounds and new methods for the degree of Polynomial Calculus proofs for other principles is another important problem. In particular, one can generate random 3CNF formulas with m clauses and n variables and when $m = 4.3n$, such formulas are believed to be hard to refute for all natural proof systems. An open problem is to prove linear degree lower bounds for such formulas. This would show that on average (as opposed to worst-case), unsatisfiable formulas (from this distribution) require large degree proofs.

5.3 Degree versus monomial size

What is the relationship between the minimal degree of a Nullstellensatz/Polynomial Calculus refutation and the minimal number of monomials in a refutation? This is analagous to pinning down exactly the relationship between the minimal Resolution clause width for a formula and the minimal Resolution proof size. Some weak results are known, establishing a connection between them, but they are far from tight [11, 9].

5.4 Representation theory and uniformity

Important work by Ajtai [1] exploits the uniform nature of standard unsatisfiable families of formulas to establish a close connection between Nullstellensatz degree lower bounds and representation theory of the symmetric group. These ideas were further developed by Krajíček[16] to obtain nonconstant degree lower bounds for the Polynomial Calculus. This line of research is quite promising and deserves further study.

5.5 Algebraic Theorem provers

Designing efficient theorem provers for the propositional calculus is an important practical question. To date, Resolution-based algorithms are the champion theorem provers although they are theoretically quite weak as proof systems. A recent challenger is the Polynomial Calculus and more specifically, using variants of the Gröbner basis algorithm to solve 3SAT [11]. This type of algorithm needs to be fine-tuned to the same extent as Resolution based methods and then rigorously evaluated on standard hard examples. On a more theoretical side, can the simulations of Resolution by PC be improved? Another very interesting question is whether or not Cutting Planes can be simulated by efficient PC proofs.

5.6 Natural proofs in proof complexity?

In a major blow to circuit complexity, [20] show that, subject to some plausible cryptographic conjectures, current techniques will be inadequate for obtaining super-polynomial circuit lower bounds. To this point, proof complexity has made steady progress at matching the superpolynomial lower bounds currently known in the circuit world. Unlike the circuit world, however, there is no analogue of Shannon's counting argument for size lower bounds for random functions, and there does not seem to be any inherent reason for Frege lower bounds (and similarly for superpolynoimal lower bounds for algebraic proofs) to be beyond current techniques. Is there any analogue of natural proofs in proof complexity?

References

[1] Ajtai, M., Symmetric systems of linear equations modulo p. Technical Report TR94-015, Electronic Colloquium in Computational Complexity, 1994.

[2] Beame, P., and Pitassi, T., "Propositional Proof Complexity: Past, Present and Future," To appear in the Bulletin of the EATCS, 1998.

[3] Beame, P., and Riis, S., More on the relative strength of counting principles. In *Proof Complexity and Feasible Arithmetics*, Beame and Buss eds., AMS, 1998.

[4] Beame, P., Impagliazzo, R., Krajíček, J., Pitassi, T., Pudĺak, P. (1995) Lower bounds on Hilbert's Nullstellensatz and propositional proofs. *Proceedings of the London Mathematical Society*, 73, 3, 1996, pp.1-26.

[5] Brownawell, D. (1987) Bounds for the degrees in the Nullstellensatz, *Annals of Mathematics* (Second Series), 126: 577-591.

[6] Buss, S., "Lower bounds on Nullstellensatz proofs via designs." In *Proof Complexity and Feasible Arithmetics*, Beame and Buss, eds., AMS, 1998, pp. 59-71.

[7] Buss, S., and Pitassi, T., The complexity of the induction principle. To appear in *JCSS*.

[8] Buss, S., Impagliazzo, R., Krajíček, J., Pudĺak, P., Razborov, S., Sgall, J., Proof complexity in algebraic systems and constant depth Frege systems with modular counting. *Computational Complexity,* 6, pp. 256-298, 1997.

[9] Ben Sasson, E., and Wigderson, A., Private communication, 1998.

[10] Caniglia, L., Galligo, A., and Heintz, J. Some new effectivity bounds in computational geometry. *Proc. 6th Int'l Conference on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Ed. T.Mora, pp. 131-151. LNCS 357, 1989.

[11] Clegg, M., Edmonds, J., and Impagliazzo, R. Using the Groebner basis algorithm to find proofs of unsatisfiability, *28th ACM STOC*, pp. 174-183, 1996.

[12] Beame, P., Cook, S., Edmonds, J., Impagliazzo, R., and Pitassi, T. The relative complexity of NP search problems, *27th ACM STOC*, pp. 303-314.

[13] Cook, S. A., and Reckhow, A. R. (1979) The relative efficiency of propositional proof systems, *J. Symbolic Logic*, 44(1):36-50.

[14] Grigoriev, D., Tseitin's Tautologies and lower bounds for Nullstellensatz proofs. Manuscript, 1998.

[15] Kollár, J. (1988) Sharp effective Nullstellensatz, *J. Amer. Math. Soc.*, 1(4):963-975.

[16] Krajíček, J., On the degree of ideal membership proofs from uniform families of polynomials over finite fields. Manuscript, 1997.

[17] Maciel, A., and Pitassi, T., On $ACC^0[p]$-Frege proofs. In *Proof Complexity and Feasible Arithmetics*, Beame and Buss eds., AMS, 1998.

[18] Pitassi, T., Algebraic propositonal proof systems. *DIMACS Series in Discrete Math. and Theoretical Computer Science,* 31, pp. 215-244, 1997.

[19] Razborov, A., Lower bounds for the polynomial calculus, To appear in *Computational Complexity.*

[20] Razborov, A., Rudich, S. Natural proofs, in *Proceedings of 26th ACM STOC*, 1994, pp. 204-213.

[21] Urquhart, A., The complexity of propositional proof systems, Survey article to appear in *Journal of Symbolic Logic.*

[22] Valiant, L. G., The complexity of enumeration and reliability problems. *SIAM J. Comput.*, 8, pp.410-421, 1979.

Toniann Pitassi
Department of Computer Science
University of Arizona
Tucson, Arizona 85719
toni@cs.arizona.edu